Journey Identity Solutions for Financial Institutions

Journey

Journey has developed the world's first identity network and platform to enable composable, frictionless, and highly secure identity experiences in the contact center. It enables customers to use the powerful sensors on smart devices to bring digital identity functions like biometrics, device data, location, history and more into the voice channel.

Journey has pre-integrated best-in-class identity capabilities, enabling banks to request, encrypt, and tokenize any identity proof, authentication, payment, document, biometric, and more to utterly change how customers and employees prove their identity for secure, fast, elegant and privacy-preserving interactions.

For example, a KYC-compliant onboarding can be completed in a minute or two, with a veracity of up to 1 in 125 million.

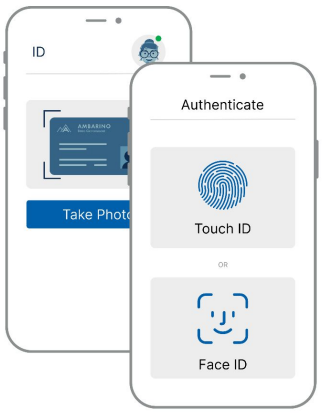
Authentication use cases can be easily composed based on the desired level of security on a spectrum from completely passive to a more secure stepped up authentication for sensitive transactions.

Because adding the digital channel to a voice call creates a significant change to the types of interactions you can now support, it has massive simultaneous impacts on user experience, security, and key contact center metrics:

- increased IVR containment
- decreased handle time
- increased first call resolution
- improved compliance stance

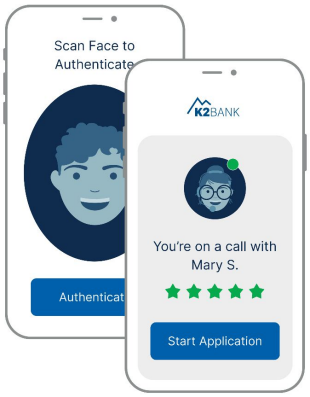
Journey's network and platform architecture works with any contact center platform, agent environment and voice or data channel.

Common Use Cases for Financial Services



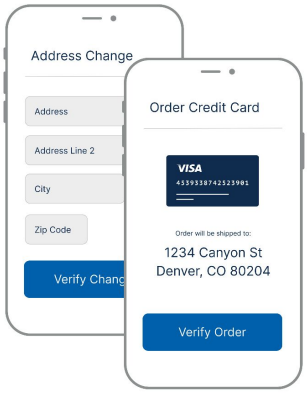
KYC-Compliant Onboarding

- Capture biometrics, document ID and all necessary data



Passwordless Authentication Across Channels

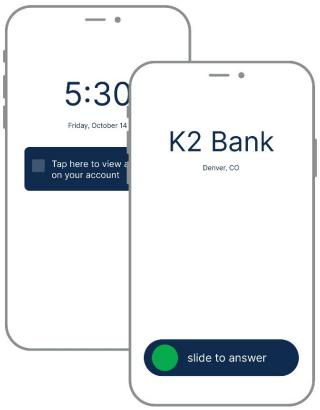
- Step Up Authentication for Loan or Credit Applications
- Frictionless authentication
- Mutual authentication



Ultra Secure Interactions

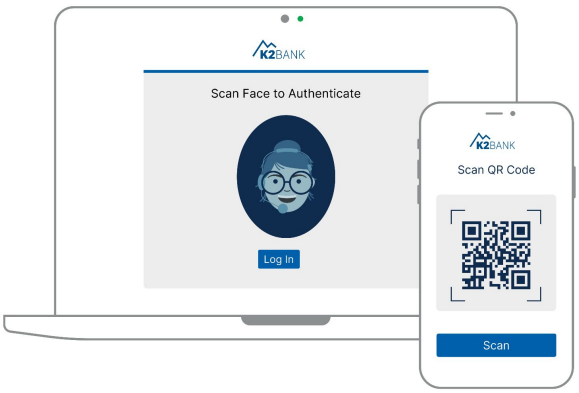
- Address or name change
- Secure Check or Credit Card orders

Common Use Cases for Financial Services (Cont'd)



Outbound Campaigns

- Fraud notifications
- Collections
- Branded Callbacks



Remote Agent and Employee Workers

- Biometric log ins
- Clean Screens

Benefits

- KYC compliant onboarding in less than 30 seconds
- Authentication in less than 2 seconds
- Completely passive authentication options
- Ultra high veracity identity proofs with veracity of 1:125 million
- High veracity identity thwarts almost all fraud attempts
- Works in all channels
- Contact center platform agnostic
- etc

Case Study

A top tier bank in the US with millions of customers takes about 1 billion calls annually in its contact center. Depending on the purpose of the call, the contact center must verify the caller's identity, consuming anywhere from 30 to 90 seconds. The customer must openly share their PII over the voice channel, which is uncomfortable on top of being highly insecure. The CC is the #1 fraud vector, so millions of dollars walk out the door monthly, and integrating new security solutions is a grueling process fraught with failure points because the bank has over 20,000 apps and use cases.

Journey was chosen as the onboarding and authentication solution because its identity network and pre-integrated platform work seamlessly with on-premise and cloud solutions across customer touch points and contact center channels (voice, chat, IVR/IVA, agent desktop, and more). The platform can leverage passive, active, biometric, and behavioral data to prove identity to a high degree of veracity in about 2 seconds, saving millions of dollars, driving huge efficiencies, and creating an elegant and modern customer experience.

Questions to Consider:

1. Do you struggle with compliance for any payment, privacy or security regulations (HIPAA, PCI, GDPR, CCPA, KYC or BSA, for example)
2. Do your agents spend more than 30 seconds authenticating callers?
3. Do you struggle with transitions between contact center channels? For example, do you require customers to authenticate each time they move from IVR to agent or agent to agent?
4. Do you know when a customer enters the contact center from a digital channel and do you have to re-authenticate them?
5. Do you take payments in your contact center?
6. Do you experience fraud in your contact center?
7. Do you have agents working from home with sensitive information on their screens?